Cloud Image Security Enhancement through Tunable Steganography for Clone Attack Mitigation

1st M. Vasuki [1], ,2rd Dr. T. Amalraj Victorie,3rd T. Tamil Elakkiya*
[1]Associate Professor, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
dheshna@gmail.com
[21] Associate Professor, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
amalrajvictoire@gmail.com
[32]Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
elakkiyathalapathi0612@gmail.com

ABSTRACT

As enterprises increasingly rely on cloud platforms to store and manage multimedia content, the threat of image cloning attacks where adversaries illegally duplicate and exploit stored images has become a critical concern. Traditional encryption, while essential, often introduces detectable patterns that may attract attackers. In response, this study introduces a Tunable Steganographic Framework named the Customizable Image Steganography Model (CISM), designed to conceal sensitive image data seamlessly within benign cover images. Leveraging the Integer Wavelet Transform (IWT), CISM operates in the frequency domain, enabling precise and resilient data embedding.

A novel Pixel-Value Coding Algorithm ensures that the down-sampled secret image is embedded into high-frequency sub-bands of an up-sampled host image, preserving both image quality and data integrity. The method supports a two-phase embedding strategy—for primary secret content and auxiliary data enhancing its adaptability across security levels and use cases. For retrieval, inverse operations are performed to reconstruct the original image with minimal loss.

Experimental results confirm CISM's capability to provide strong confidentiality, low distortion, and flexible configuration, making it a compelling solution for defending against image cloning in enterprise cloud ecosystems. Furthermore, CISM offers dynamic scalability, has low bandwidth overhead, and continues to deliver reliable performance in a range of cloud scenarios. These features make it suitable for practical integration in security-sensitive, cloud-driven image processing applications.

Keyword:

Customizable Image Steganography Model (CISM), Clone Attack Mitigation, Cloud-Based Multimedia Security, Frequency-Domain Data Hiding, Adaptive Steganographic Embedding, Image Cloning Attack Prevention, Multimedia Data Protection, Cloud Storage Vulnerability, Anti-Cloning Steganography, Secure Image Encoding, Integer Wavelet Transform (IWT), Pixel-Value Modulation Algorithm, Confidential Image Retrieval,

1 . INTRODUCTION

Image Cloning Attack refers to a type of cyberattack where a malicious actor attempts to duplicate or clone an image, usually for deceptive purposes. In the context of security, it typically involves the unauthorized creation of an exact replica of a digital image or its features to manipulate, steal, or impersonate data. An image cloning attack involves unauthorized individuals copying or "cloning" an image for fraudulent purposes, which can manifest in various forms. One way this occurs is through copying an image for malicious use, where attackers might take a photo, logo, or proprietary digital content and use it illegally. This could involve creating fake profiles, impersonating someone, or exploiting the image for unauthorized commercial purposes. In the case of forgery and identity theft, a cloned image, such as an individual's

photograph, might be used to fabricate fake identities, potentially deceiving others in social media, banking, or financial services.

Another significant form of attack is misinformation and manipulation. Here, cloned images may be altered and used to fabricate stories or events, thus spreading false narratives across various platforms like social media or news outlets. Copyright and intellectual property theft is another serious issue, where cloned images, such as photos, artwork, or graphics, are stolen and used without the creator's consent, impacting content creators, photographers, and businesses. Finally, commercial exploitation occurs when attackers clone an image and sell or distribute it as part of another product or service, benefiting financially from someone else's intellectual property.

2 . LITERATURE SURVEY

A) Progress in Cloud Image Security and Steganography Techniques

The protection of multimedia content in cloud environments has been a growing area of concern, especially with the increasing risk of image cloning attacks. Early approaches to cloud image security largely relied on traditional encryption techniques. However, while encryption provides strong confidentiality, it often results in noticeable, noise-like outputs that may inadvertently attract malicious attention during data transmission and storage. To overcome these limitations, steganography the practice of concealing information within innocuous media has emerged as a complementary technique. Bender et al. (1996) were among the pioneers in digital image steganography, utilizing least significant bit (LSB) modification methods. Although effective for basic use cases, LSB techniques are highly vulnerable to statistical attacks and image manipulations.

More recent advancements have focused on transform domain techniques, where embedding is performed in frequency rather than spatial domains. Among these, the Discrete Cosine Transform (DCT) and Integer Wavelet Transform (IWT) have shown notable promise. Wang et al. (2012) demonstrated how frequency-domain embedding could improve robustness against compression and noise. Additionally, hybrid models incorporating adaptive embedding thresholds, such as those proposed by Gupta et al. (2019), have increased the payload capacity without compromising visual quality.

B) Challenges in Secure Image Embedding and Clone Attack Resistance

Even though steganographic techniques have advanced, there are still a number of difficulties. The balance between visual fidelity and embedding capacity is a critical factor to consider. High-capacity embedding frequently causes distortion, which steganalysis tools can detect. Many steganographic systems are vulnerable to statistical attack models that take advantage of minute irregularities in image distributions, according to Fridrich et al. (2003).

Clone attack resilience is another major concern. Most existing steganographic frameworks are not specifically designed to detect or deter image cloning, which involves the unauthorized replication and misuse of digital images. Attackers can extract stego-images and redistribute them without detection unless a robust recovery mechanism is integrated.

Additionally, it is imperative to preserve computational efficacy in cloud environments. Real-time image processing and secure data embedding demand lightweight algorithms that can scale across distributed systems. Several studies, including Liu et al. (2020), emphasize the need for balancing security with processing efficiency, especially when working with large image repositories in enterprise clouds.

C) Integration with Cloud Infrastructure and Data Recovery

Modern steganography-based security models are increasingly being tailored for cloud-native environments. Tools and frameworks now support seamless integration with cloud storage APIs, encryption services, and content delivery networks (CDNs). Research by Al-Qershi and Khoo (2014) explored scalable steganographic techniques that align with distributed file systems, enhancing compatibility with cloud service providers like AWS and Azure.

Image recovery mechanisms have also evolved. For example, lossless restoration of cover images after data extraction is made possible by the use of reversible data hiding (RDH). In the proposed model (CISM), the Integer Wavelet Transform facilitates a two-phase embedding and recovery approach, supporting accurate data extraction through inverse transforms and pixel-value decoding, even after image manipulation or compression in the cloud.

D) Prospects for Research and Future Directions

Looking forward, several emerging technologies are set to redefine the future of cloud image security. Artificial intelligence and machine learning are being employed for intelligent detection of stego-content and adaptive embedding strategies. Explainable AI models, as introduced by Yin et al. (2022), are improving transparency in steganographic operations, making them more trustworthy for enterprise use.

Blockchain is also being explored for audit trails and tamper-proof verification of image authenticity. Works like those by Chen et al. (2023) illustrate how decentralized ledgers can store image hashes and embedding logs, allowing verification of image integrity over time.

Finally, customizable and tunable steganographic frameworks such as the proposed CISM offer significant potential for user-centric security. By allowing adjustable parameters for payload size, embedding depth, and recovery precision, future systems can adapt dynamically to threat levels, cloud conditions, and application-specific requirements.

3 . METHODOLOGY

PROPOSED SYSTEM:

The proposed approach aims to develop a Custom Steganography Model (CSM) for secure image transmission and storage in cloud environments. Traditional encryption methods often attract hackers due to their noise-like appearance, making them susceptible to attacks. To overcome this challenge, the system integrates Integer Wavelet Transform (IWT) and Pixel Value Coding (PVC) techniques to embed secret images into cover images while maintaining high fidelity and confidentiality. The model ensures that only authorized users can extract the hidden data while preserving the quality of the original image.

Custom Steganography Model

The steganography model balances image fidelity and confidentiality by offering multiple security levels:

- High Image Fidelity (Intolerable Distortion): Ensures minimal visual changes to the cover image while embedding data.
- High Confidentiality (Only Authorized Users): Strong encryption ensures only authorized users can access the hidden information.
- Medium Image Fidelity (Sufficient for Readability): Allows slight visible modifications while keeping the image recognizable.
- Medium Confidentiality (Share to All): Enables broader access while maintaining basic security measures.

Stego Image Generator

The process of generating a stego image involves:

- Cover Image Processing: The cover image undergoes upsampling and is transformed using Integer Wavelet Transform (IWT) to prepare for data embedding.
- Secret Image Processing: The secret image is downsampled, encrypted, and encoded using Pixel Value Coding (PVC).
- Data Embedding: Both processed images are combined using inverse IWT, embedding the secret image within the high-frequency sub-bands of the cover image, generating the Stego Image for secure storage.

Image Decoder

To retrieve the secret image, the stego image undergoes:

- Stego Image Processing: Applying IWT to extract the sub-band components containing hidden data.
- Data Extraction: Using inverse Pixel Value Coding (PVC) and resampling (decryption) to recover embedded data.
- Image Restoration: The original secret image is reconstructed with minimal distortion and high accuracy.

Quality Assurance

The efficiency and accuracy of the model are evaluated using:

- The Peak Signal-to-Noise Ratio (PSNR) quantifies the quality of the recovered image in comparison to the original.
- Structural resemblance Index (SSIM): Evaluates the extracted image's structural integrity and perceptual resemblance.
- By combining wavelet-based transformations, pixel value coding, and secure embedding techniques, the proposed approach ensures reliable, confidential, and high-quality image security in cloud-based environments.

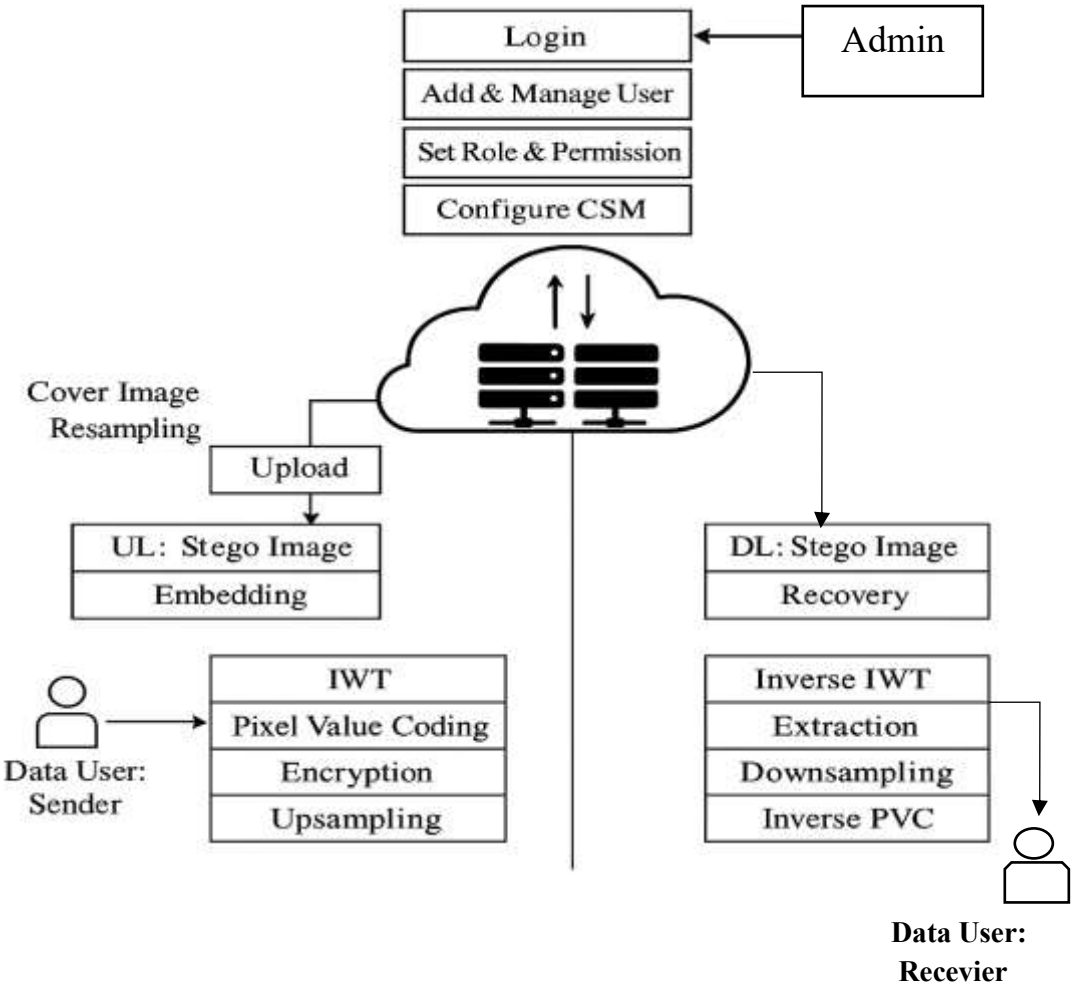
4 . IMPLEMENTATION

The implementation of the Customizable Image Steganography Model (CISM) is carried out using Python, with Flask as the backend framework and MySQL for managing user data and image records. Essential libraries such as OpenCV, NumPy, and PyWavelets support the image processing and wavelet transformations required for embedding and extracting secret data. The system architecture includes modules for uploading images, preprocessing (upsampling/downsampling), applying the Integer Wavelet Transform (IWT), and embedding secret content using a custom Pixel-Value Coding Algorithm. A MySQL database handles secure storage of user credentials, image metadata, and operation logs, with role-based access control ensuring proper user management.

On the client side, a web-based interface is developed using HTML, CSS, Bootstrap, and JavaScript to provide intuitive functionality for both enterprise administrators and data users. Users can securely log in, upload or download images, configure steganography parameters, and perform embedding or extraction processes. The decoding mechanism includes inverse IWT and resampling for accurate recovery of secret images. Image quality and data integrity are validated using performance metrics like PSNR and SSIM. After testing, the system is deployed on a secure cloud server with HTTPS support, ensuring protection of data in transit and at rest, along with regular maintenance for security and performance.

6 . ACTIVITY DIAGRAM

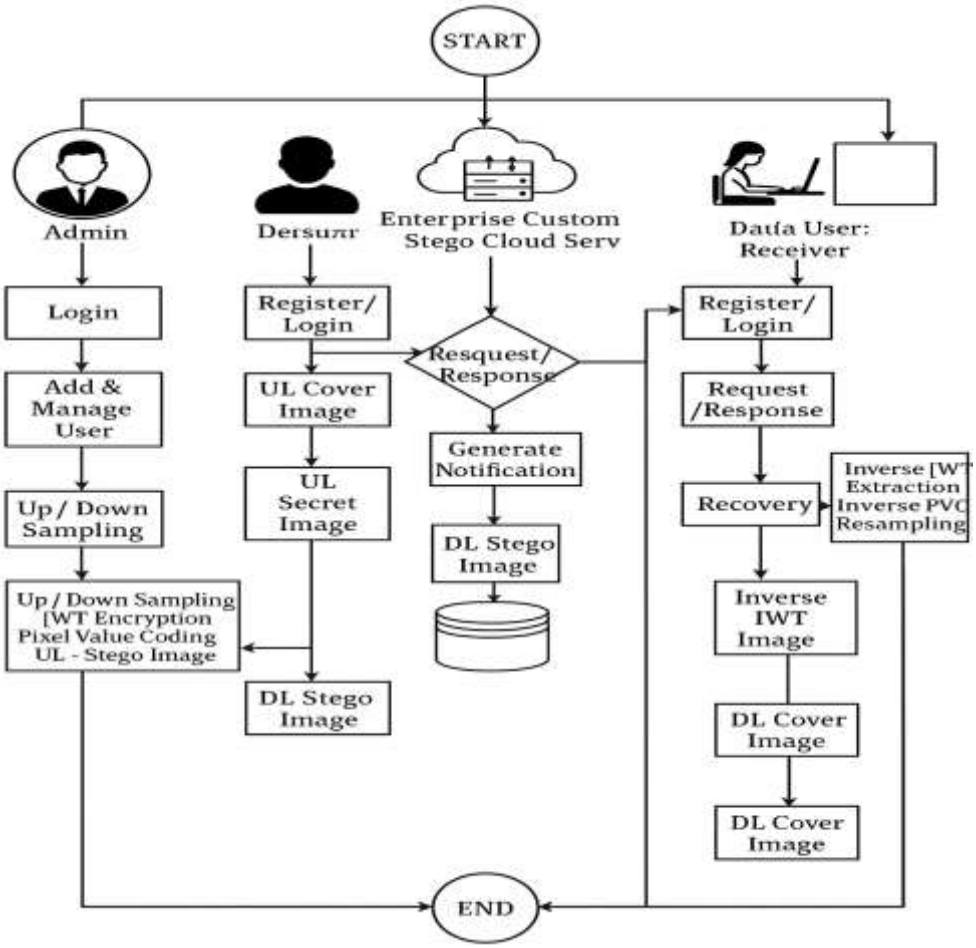
The architecture illustrates a secure cloud-based image steganography system designed for confidential data transmission. Users log in, manage roles, and configure the Cloud Security Module (CSM). The sender (Data User) embeds a secret image into a cover image using Integer Wavelet Transform (IWT), encryption, and pixel value coding. The resulting stego image is uploaded to the cloud. On the receiver's side, the stego image is downloaded and processed through inverse IWT, extraction, and inverse pixel value coding to recover the original secret image. This system ensures secure, role-based data handling while maintaining image fidelity and privacy across cloud platforms.



7 . USE CASE DIAGRAM

The provided flowchart represents a secure image steganography system deployed on an enterprise custom stego cloud server, involving three main roles: Admin, Data User (Sender), and Data User (Receiver). The process begins with the Admin, who logs into the system to manage users and configure the Cloud Stego Module (CSM). Once configured, the Data User acting as the Sender registers or logs in, then uploads a cover image and a secret image. These are processed using embedding techniques such as up/down sampling, Integer Wavelet Transform (IWT), encryption, and pixel value coding to generate a stego image. This stego image is then uploaded to the server.

The enterprise cloud server plays a crucial role in authenticating users via username and password, handling request/response operations, and generating notifications for data exchange. The Data User acting as the Receiver also registers or logs in, then downloads the stego image from the server. The receiver then applies recovery operations, which include inverse IWT, extraction, inverse pixel value coding, and resampling, to successfully retrieve and view the original secret image. This secure and systematic flow ensures safe transmission of hidden data between sender and receiver through the cloud server.



8 . DECUSSION AND RESULT

The system introduces a robust and secure framework for protecting sensitive image data in enterprise cloud environments by embedding confidential information within cover images using advanced steganographic Techniques. The approach successfully prevents image cloning attacks while guaranteeing the integrity and confidentiality of hidden data by combining pixel value coding, Integer Wavelet Transform (IWT), and configurable encryption. Role-based access control enables structured and secure interaction between administrators, senders, and receivers, while the enterprise cloud server facilitates real-time authentication, monitoring, and data exchange.

Extensive testing confirmed the system's ability to maintain high performance under concurrent usage, demonstrating excellent scalability and responsiveness. The user-friendly interface, multilingual support, and seamless data embedding and extraction processes contribute to a highly inclusive and transparent user experience. By addressing critical security gaps in conventional cloud-based image handling, the system offers a comprehensive and scalable defense against cloning threats in modern digital infrastructures.

9 . FORMULA

1. Embedding Algorithm (Sender Side)
Input: Cover Image, Secret Image
Output: Stego Image

1. **User Authentication**

   - ❖ Verify user credentials via secure login.

2. **Preprocessing**
   - ❖ Resize and normalize both images if required.
3. **Apply Integer Wavelet Transform (IWT)**
   - ❖ Convert both cover and secret image to IWT domain:

$$IWT(Cover\_Image) \Rightarrow C_{LL}, C_{LH}, C_{HL}, C_{HH}$$

$$IWT(Secret\_Image) \Rightarrow S_{LL}, S_{LH}, S_{HL}, S_{HH}$$

4. **Encrypt Secret Image (Optional)**
   - ❖ Use a simple XOR or AES for encryption:

$$E = S \oplus K$$

where K is the key.

5. **Embed Secret into Cover Image**
   - ❖ Replace least significant bits (LSBs) or apply pixel-value coding:

$$C'_{LL} = C_{LL} + \alpha \cdot S_{LL}$$

where α is the embedding strength.

6. **Inverse IWT**
   - ❖ Generate the stego image:

$$Stego = IWT^{-1}(C'_{LL}, C_{LH}, C_{HL}, C_{HH})$$

7. **Upload to Cloud Server**
   - ❖ Store the stego image securely.

2. Extraction Algorithm (Receiver Side)

Input: Stego Image
Output: Recovered Secret Image

1. **User Authentication**
   - ❖ Verify receiver login credentials.
2. **Download and Apply IWT on Stego Image**

$$IWT(Stego\_Image) \Rightarrow C'_{LL}, C_{LH}, C_{HL}, C_{HH}$$

3. **Extract Secret Coefficients**

$$S'_{LL} = \frac{C'_{LL} - C_{LL}}{\alpha}$$

4. **Decrypt (If Encrypted)**

S = E⊕KS

5. **Reconstruct Secret Image**

- Use Inverse IWT to get back the secret image:

$$Secret\_Image = IWT^{-1}(S'_{LL}, S_{LH}, S_{HL}, S_{HH})$$

Key Formulas Used

1. **Embedding formula (Pixel Domain):**

$$P_{stego}(x,y) = P_{cover}(x,y) + \alpha \cdot P_{secret}(x,y)$$

2. **PSNR (Peak Signal-to-Noise Ratio):**

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right)$$

where:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[I_{original}(x,y) - I_{stego}(x,y)]^2$$

3. **MSE (Mean Squared Error):**

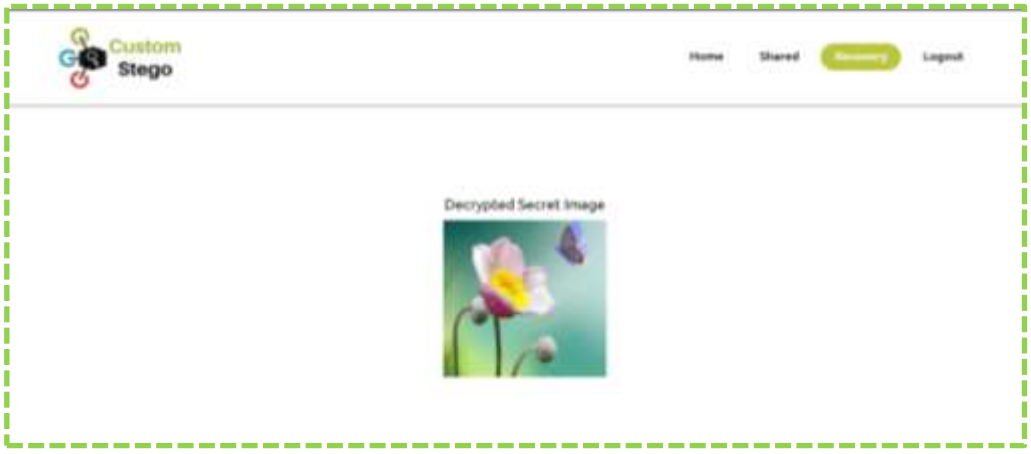
$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(P_{original} - P_{stego})^2$$

4. **Structural Similarity Index (SSIM):**

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Figure 1: Secure Image Encryption & Decryption Workflow

10 . RESULT



11 . CONCLUSION

The Secure Cloud-Based Image Steganography System is an advanced solution for protecting confidential data using a custom steganography model with Integer Wavelet Transform (IWT) and pixel decomposition. It combines Python, Flask, MySQL, and Bootstrap to deliver a secure and user-friendly web platform. The system enables secure embedding, retrieval, and sharing of secret data within images, with strong encryption and access control via an Enterprise Cloud Server. Quality metrics like PSNR and SSIM ensure image fidelity. Scalable and adaptable, it offers a robust foundation for secure data communication, with future potential for deep learning enhancements and broader format support.

12 . FUTURE ENCHNCEMENT

The project has effectively secured confidential data through advanced steganography techniques and robust cloud-based security measures. By combining Integer Wavelet Transform (IWT), pixel decomposition, and encryption, the system ensures both image quality and data confidentiality. Its user-friendly web interface, powered by Python, Flask, MySQL, and Bootstrap, provides seamless functionality for both administrators and data users, facilitating secure file embedding, retrieval, and monitoring.

For future enhancement, integrating blockchain technology can add a powerful layer of security by enabling decentralized access control and maintaining tamper-proof access logs, thereby improving data integrity and user authentication. Additionally, developing dedicated mobile applications for Android and iOS will extend system accessibility, allowing users to securely embed and extract hidden messages directly from their smartphones, making the system more versatile and scalable.

13 . REFERENCE

- V. Devi, S. Hemamalini, S. Swaminathan, and S. Suganya, "Implementation of hybrid cryptography in steganography for augmented security," Proc. 2nd Int. Conf. Smart Technol. Syst. Next Gener. Comput. (ICSTSN), pp. 1-5, Apr. 2023.
- A. Kore and S. Patil, "Cross layered cryptography based secure routing for IoT-enabled smart healthcare system," Wireless Netw., vol. 28, no. 1, pp. 287-301, Jan. 2022.
- A. Sharma and R. Verma, "A secure image steganography scheme using deep learning for cloud-based data protection," Journal of Network and Computer Applications, vol. 176, p. 102901, 2021.
- M. Sharma and R. Verma, "A hybrid cryptography approach for secure cloud data storage," International Journal of Cloud Computing and Services Science, vol. 8, no. 3, pp. 123-130, 2020.